Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: [141231999-4999-01]

National Cybersecurity Center of Excellence (NCCoE) Situational Awareness Use Case for the Energy Sector

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide products and technical expertise to support and demonstrate security platforms for situational awareness for the energy sector. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the Energy sector program. Participation in the use case is open to all interested organizations.

DATES: Interested parties must contact NIST to request a letter of interest. Letters of interest will be accepted on a rolling basis. Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than [PLEASE INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. When the use case has been completed, NIST will post a notice on the NCCoE energy sector program website at http://nccoe.nist.gov/energy announcing the completion of the use case and informing the public that it will no longer accept letters of interest for this use case.

ADDRESSES: The NCCoE is located at 9600 Gudelsky Drive, Rockville, MD 20850. Letters of interest must be submitted to Energy_NCCoE@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Organizations whose letters of interest are accepted in accordance with the Process set forth in the SUPPLEMENTARY INFORMATION section of this notice will be asked to sign a Cooperative Research and Development Agreement (CRADA) with NIST. A CRADA template can be found at: http://nccoe.nist.gov/node/138.

FOR FURTHER INFORMATION CONTACT: Jim McCarthy via email at Energy_NCCoE@nist.gov; or telephone 240-314-6816; National Institute of Standards and Technology, NCCoE; 9600 Gudelsky Drive; Rockville, MD 20850. Additional details about the Energy Sector program are available at http://nccoe.nist.gov/energy.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into a Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the Situational Awareness use case for the Energy Sector. The full use case can be viewed at:

http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Situational_Awareness.pdf

Interested parties should contact NIST using the information provided in the FOR FURTHER INFORMATION CONTACT section of this notice. NIST will then provide each interested party with a letter of interest, which the party must complete, certify that it is accurate, and submit to NIST. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the use case objective

or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed below up to the number of participants in each category necessary to carry out this use case. However, there may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into a consortium CRADA with NIST. NIST published a notice in the Federal Register on October 19, 2012 (77 FR 64314) inviting U.S. companies to enter into National Cybersecurity Excellence Partnerships; (NCEPs) in furtherance of the NCCoE. For this demonstration project, NCEP partners will not be given priority for participation.

Use Case Objective: To improve the security of operational technology, energy companies need mechanisms to capture, transmit, analyze and store real-time or near-real-time data from industrial control systems (ICS) and related networking equipment. With such mechanisms in place, energy sector providers, owners and operators can more readily detect anomalous conditions, take appropriate actions to remediate them, investigate the chain of events that led to the anomalies and share findings with other energy companies. Obtaining real-time and near-real-time data from networks also has the benefit of helping to demonstrate compliance with information security standards.

Requirements: Each responding organization's letter of interest should identify which security platform components or capabilities it is offering. Components are listed in

section five (for reference, please see link in PROCESS section above) of the Situational Awareness for the Energy Sector use case and include, but are not limited to:

1. Security incident and event management (SIEM) or log analysis software
2. ICS equipment, such as remote terminal units (RTUs), programmable logic controllers (PLCs), and relays, along with associated software and communications equipment (e.g., radios, encryptors)
3. "Bump-in-the-wire" devices for augmenting operational technology (OT) with encrypted communication and logging capabilities
4. Software for collecting, analyzing, visualizing and storing operational control data (e.g., historians, outage management systems, distribution management systems, human-machine interfaces)
5. Products that ensure the integrity and accuracy of data collected from remote facilities

Each responding organization's letter of interest should identify how their products address one or more of the following desired solution characteristics in section two (for reference, please see link in PROCESS section above) of the Situational Awareness for the Energy Sector use case:

1. Data visualization and analysis capabilities that help dispatchers and security analysts view control system behavior, network security events, and physical security events as a cohesive whole
2. Analysis and correlation capabilities that help dispatchers and security analysts understand and identify security events and predict how those events might affect control system operation
3. Scalability sufficient to meet the needs of a large metropolitan utility
4. Mechanisms that ensure the accuracy and integrity of data collected from remote facilities

5. Ability to collect logs, traffic, and operational data from a variety of sources, including servers, ICS equipment, networking equipment, security appliances, issue tracking systems, and mobile devices

6. Ability to allow dispatchers and security analysts to easily automate common, repetitive investigative tasks

7. Built-in information sharing capabilities that allow dispatchers and security analysts to easily share and acquire new threat indicators, correlation rules, mitigations, and investigative techniques

8. Customizable interfaces that allow users to tailor the system to meet specific business needs

9. Automated report generation to aid utilities in demonstrating compliance with relevant standards

10. Intuitive user interfaces that are appropriate for utility dispatchers with limited network security expertise or security analysts with limited expertise in electric power

Responding organizations need to understand and, in their letters of interest, commit to provide:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components
2. Support for development and demonstration of the Situational Awareness use case for the Energy Sector in NCCoE facilities which will be conducted in a manner consistent with Federal requirements (e.g., FIPS 200, FIPS 201, SP 800-53, and SP 800-63)

Additional details about the Situational Awareness for the Energy sector use case are available at:

http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_ES_Situational_Awareness.pdf

NIST cannot guarantee that all of the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the consortium agreement in the development of the Situational Awareness for the Energy sector capability. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each prospective participant will train NIST personnel as necessary, to operate its product in capability demonstrations to the energy community. Following successful demonstrations, NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the Situational Awareness for the Energy sector use case. These descriptions will be public information.

Under the terms of the consortium agreement, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of the Situational Awareness for the Energy sector capability will be announced on the NCCoE Web site at least two weeks in advance at http://nccoe.nist.gov/. The expected outcome of the demonstration is to improve situational awareness across an entire energy sector enterprise. Participating

organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE Web site http://nccoe.nist.gov/.

Kevin A. Kimball
NIST Chief of Staff

[FR Doc. 2015-01844 Filed 01/30/2015 at 8:45 am; Publication Date: 02/02/2015]